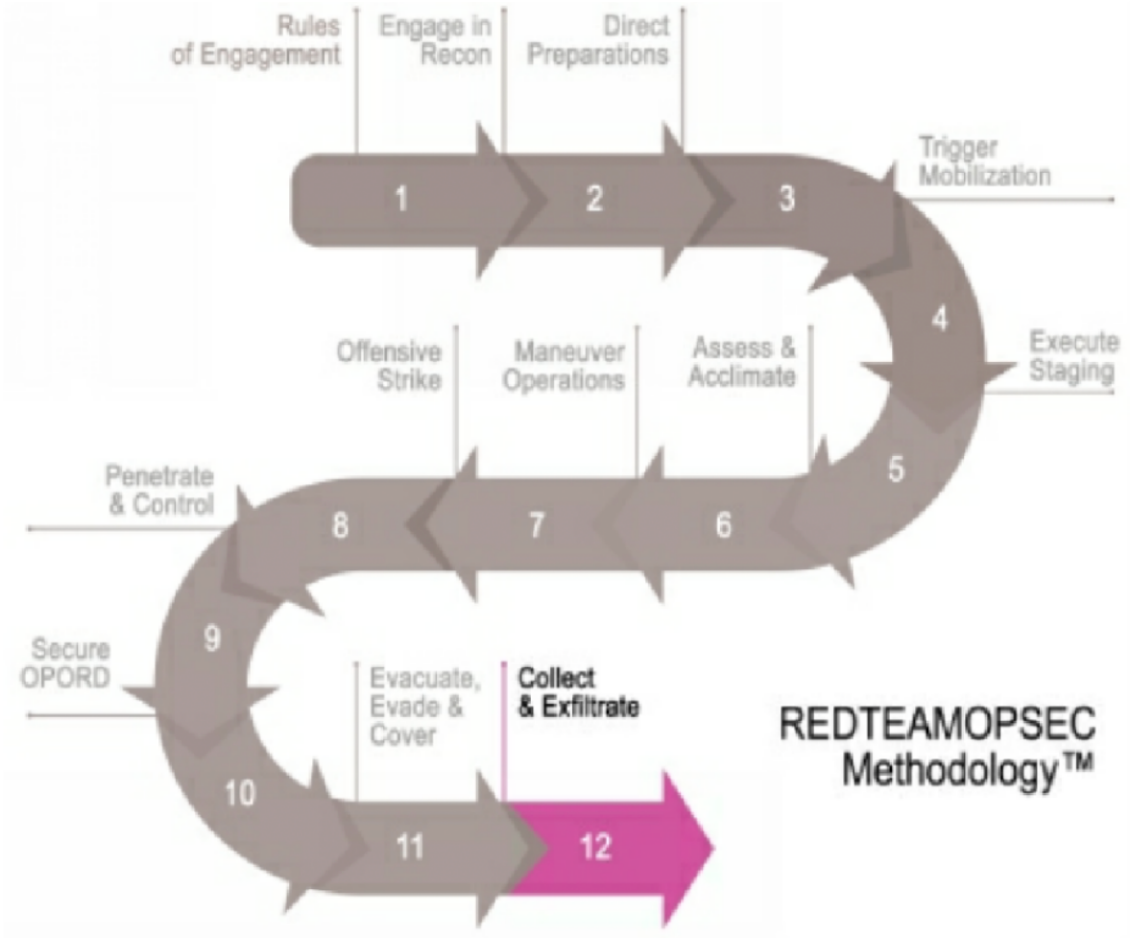
COLLECT & EXFILTRATE

The alpha team radios the red team leader, "I think we've been made. We're behind a dumpster outside the entrance, but a car has its l.ights on us, and we can't move." Then, the engine and headlights stop. Two men exit the car and enter through the loading dock door. The alpha team is relieved they weren't spotted. The men were dressed as the deaning crew. They must be back from a late-night break. The alpha team radios a SITREP to the red team leader and she orders them to proceed to the rally point. As they move out, one operator remarks quietly to the other about how noticeably active the location is compared to the recon phase.

The bravo team, meanwhile, had nearly reached the waiting van at the rally point until the red team leader radioed for all teams to hunker down. Just in front of the van, a few people walking down the sidewalk stopped to talk and were soon joined by a car who pulled up beside them. The bravo team drops to the ground a mere thirty feet away. The alpha team catches up with bravo team and drops down next to them. Both alpha team and bravo team have collected at the rally point but are unable to enter the van without being seen.

Realizing the bystanders wouldn't be going anywhere soon, the red team leader calls for the operators to low crawl to the rear of the van facing away from the small crowd. One by one they quietly crawl to the van and make entry through an open door to the back. Once the team is collected, they perform a quick equipment check to make sure nothing has been left behind. All operators crouch down out of sight of the van's windows as the red team leader fires up the van and they calmly pass the crowd and exfiltrate the target.



Collect & Exfiltrate Phase

The story at the beginning of this chapter is not all that far off from what happens during actual operations. What is important to take into account is that exiting a target is more than just walking out. Exfil takes planning, and it takes skill when things go sideways. Remember that most physical red team operations are not considered fully executed until the entire team exits the target cleanly. That's when the red team leader hits the gas in the getaway van with the entire team in tow.

A proper exit that supports a fully executed red team operation is one that happens in two generic stages: **Collect** and **Exfiltrate**. Let's take a closer look.

Collect

There are so many opportunities to accidentally leave behind equipment at the target and misplace or forget evidence altogether during an operation. I shoulld know. I've made these mistakes myself, and it nearly cost me the operation. I was gloating a little back at the hotel after completing what I thought was a successful mission inside a secure substation yard. Then a shockwave hit me when I realized I didn't have my Shove-it tool. I looked everywhere for it. After some thought, I was pretty certain I dropped it after climbing over one of four barbed-wire fences. In fact, I was even more certain it was probably inside the inner-most fence closest to the building we broke into, along a path heavily used by its employees. It was not a proud moment.

In this stage, I hope to provide guidance on how to properly collect evidence, equipment, and rally with fellow operators for a successful mission.

Evidence

An example of a bag for collecting evidence

A fair percentage of physical red team operations I have been privy to have included the capture of physical evidence. This is unlike a flag, which is a designated object an operator sets out to acquire.

Evidence might be a sticky note with root credentials, a document with confidential information, or sometimes an untethered laptop. Evidence is a security risk an operator happens upon by chance that she finds during execution and is found to be relevant to the nature of the mission objective. For example, an untethered laptop would be taken as evidence if the

company's concern is theft. Confidential documents would be taken if the company is concerned with unauthorized data disclosure. Of course, how this evidence is captured is entirely dependent upon the RoE. But it is fair to say that most often the evidence will be physically taken with the operator as opposed to only being photographed.

In short, red teamers in an operation that allows for the physical acquisition of evidence must plan for it by having adequate storage on their person to accommodate the evidence they find.

Equipment

My story about losing a piece of equipment is a real threat to red teamers, and it has dire consequences. Recall from the "Execute Staging" chapter where I advised red teamers to securely pack their gear to prevent it from falling out. This advice applies to every time an operator pulls a tool from their pack and replaces it.

An equipment check should be conducted at this point to prevent leaving something behind and raising alarms by anyone who sees it. In my previous example, I left behind a Shove-it tool. This piece of equipment looks a lot like a Slim Jim used in years past to break into cars. A giant wrench would have been thrown into our entire operation had anyone noticed it laying around near the entrance.

To reduce the chances of accidentally leaving equipment behind, I recommend making a cheat sheet of packed gear and where each piece of equipment is held.

PACKED GEAR						
Bag	**Large Compartment**	**Front Pouch**	**Left Pouch**	**Right Pouch**	**Bottom**	**Top Zipper**
Tactical Backpack	Under-the-door-tool	Laptop	LED headlamp	PlugBot, Shove-it, pick set	Small flashlight	USB drive

Packed gear cheat sheet

I almost always use the same tactical backpack and almost always put the same pieces of gear into the same compartments. But even as a

seasoned red teamer, I know the anxiety that comes about in the midst of an operation, and that will cause mistakes. A small printed copy of the cheat sheet is useful in ensuring pieces of equipment are not accidentally left behind.

Operators

This brief but necessary step is more about communication than anything. It's imperative all operators know it is time to make for the rally point, to what location if it has changed, and if there are any hazards to consider. From the story earlier in this chapter, the red team leader gave the authorization for the alpha team to head to the rally point Later in the story, the red team leader communicated concerns about a crowd gathering near the rally point. As a result, a slight deviation from the original plan was necessary in order to make a dean exit.

Essentially, this step is here to ensure the operators are able to collect at the rally point safely and make a clean exit. The onus for this step falls mostly on the red team leader. But it is important for the red teamers to communicate and coordinate similarly to support a fully executed operation.

Exfiltrate

The term exfiltrate is defined as the process of withdrawing from a place or stealing sensitive information from a computer. As you might've already guessed, the REDTEAMOPSEC methodology applies directly to the physical withdraw from a place. But there is a fuzzy line between physical red teaming and the exfiltration of electronic data.

Unfortunately, many physical red team operations today do not cross into the cyber realm to also include ethical hacking tactics. Testing is often compartmentalized to physical security without regard for how physical security vulnerabilities also impact cyber vulnerabilities and personnel vulnerabilities. To combat this, my company RedTeam Security created an approach called Full-Force Red Teaming. This is a more complex issue to

be covered in this chapter. For the sake of brevity, please refer to the final section of this book titled, "Full-Force Red Teaming."

Flags

I've used the term flag throughout this book. Let me take a moment to expand on it some. The term flag is derived from a game called Capture the Flag (CTF). It is a traditional outdoor game where two teams each have a flag (or another marker), and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.

As you can see, our use of the term flag is loosely based upon capturing an object from our client and the similarities tend to end there. A flag can be anything and usually ranges from a piece of old equipment to a physical document and everything in between.

Operators will certainly know which flags need to be captured and must plan for it accordingly. Keeping track of them during an operation is usually not difficult since there are generally only one to three flags per target. Operators can create a cheat sheet, similar to one used for packed equipment, to better manage flags captured if necessary.

Rally Point

The rally point is the final destination for red teamers once their mission objectives have been met or for other reasons as deemed necessary by the red team leader. For most teams, the rally point is a location near the target but far enough away to go unnoticed from employees and most casual passersby.

This is the last leg of the operation. The red team leader coordinates the effective and efficient exfiltration of the team, ideally leaving nothing and no one behind.

Red team leader at the rally point

presumably inside the vehicle, the red team leader must take time to conduct the following before declaring mission completion. Please have a look at the following considerations. Considerations before declaring mission success:

- Roll call. Are all red teamers present?
- Do red teamers have all of their equipment? Was anything left behind?
- Can red teamers re-attest they've successfully accomplished their mission objectives?
- Are flags and evidence captured present?

If these criteria are met to the red team leader's satisfaction, the mission can be considered complete. At this point in time, a proper team exfil is in order and the team can now physically leave the premises. The red team leader must immediately communicate the status of the operation to the

designated stakeholders by phone, email, or face-to-face, whichever communication medium was agreed upon.

With the whole team in the vehicle, it's usually right about now when the air becomes filled with the sound of enthusiastic conversations and stories of close calls. Before too much time passes, I highly recommend all operators scribble notes about the operation, noting important times and events. This should happen immediately, even while still in the vehicle. As the minutes and hours wear on, details start to become fuzzy. So **it's important** to capture these tidbits before they're gone from memory.

Team Debrief

At the earliest convenience, the team should meet to momentarily debrief and document a rough timeline of events. I suggest constructing the timeline on the same night or day. I'll admit this is one of my least favorite things to do in the middle of the night after a long day. However, specific details concerning times and events are usually the first to escape from everyone's memory, so it's best to do it as soon as possible.

When the team is rested and more productive, a proper debrief should be conducted and the timeline should be formalized. I suggest the red team leader should interview each team member to support the development of the timeline. During this process, all operators should turn in their videos/photos to the red team leader along with any flags or evidence captured.

The debrief efforts will ultimately support the development of an initial. draft of the physical red team operation report. My hope is the REDTEAMOPSEC methodology is one that will prove to be useful to you and your team in all aspects of physical red team operations.